VIRGINIA DEPARTMENT OF
SOCIAL SERVICES

PRIVACY POLICY and PROGRAM MANUAL

Prepared By:
Information Security and Risk Management

Date Document Prepared:
September 2016

Publication Version Control

Publication Version Control: It is the user's responsibility to ensure they have the latest version of this publication. Questions should be directed to the Virginia Department of Social Services (VDSS) Chief Information Security Officer (CISO) within the Information Security and Risk Management (ISRM) Office. The VDSS CISO will issue an agency-wide Broadcast and post the revised publication version on the Services.Programs.Answers.Resources.Knowledge (SPARK) Intranet, and provide an email announcement to division/directorate/office/district/region and Local Departments of Social Services (LDSS) Security Officers as well as other parties the VDSS CISO considers being interested in the change.

This chart contains a history of this publication's revisions.

Version	Date	Comments
Original	June 1, 2016	
Revision 1	September 2016	Updated Code of Virginia hyperlinks.

Review Process: The VDSS CISO and staff of the ISRM Office contributed to the review of this publication. All comments were carefully evaluated, and individuals that provided comments were notified of the actions taken.

PREFACE

Subject

The VDSS Privacy Policy and Program Manual

Effective Date: *June 1, 2016*

Authority

The policies described in this document are based on requirements found in the following codes, policies, regulations, laws, standards, and guidelines:

45 CFR §155.260, Privacy and security of personally identifiable information.

Code of Virginia, § 2.2-2005, et. seq.
Powers and duties of the Chief Information Officer "CIO" Virginia Information Technologies Agency, "VITA"

Code of Virginia, § 2.2-2009, et. seq.
Additional duties of the CIO relating to security of government databases

Code of Virginia, § 2.2-2827, et. seq.
Restrictions on state employee access to information infrastructure

Code of Virginia, § 2.2, Chapter12
Department Human Resource Management, DHRM

Part C: Minimum Acceptable Risk Standards for Exchanges (MARS-E), Version 2.0.

Other References

VDSS Information Security Policy and Program Guide (.pdf)

Purpose

The purpose of this policy is to create a prescriptive set of processes and procedures, aligned with applicable federal and Commonwealth of Virginia (COV) Information Technology (IT) security policy and standards, to ensure the Virginia Department of Social Services (VDSS) develops, disseminates, and updates the VDSS Privacy Policy and Program Manual. This policy and procedure establishes the minimum requirements for the VDSS Privacy Policy and Program.

Scope

This policy applies to:

All *individuals* (VDSS employees, LDSS employees, contractors, vendors, volunteers, student interns, work experience personnel, and other persons and organizations including the Virginia Department of Medical Assistance Services [DMAS]) who have a need to use VDSS-sponsored Internet, email, other electronic communications VDSS-related information or information processing systems.

All information and information processing systems associated with other organizations which VDSS uses, including but not limited to, the Social Security Administration (SSA), the Virginia Department of Taxation (TAX), the Internal Revenue Service (IRS), the Department of Motor Vehicles (DMV), and the Virginia Employment Commission (VEC).

Table of Contents

AP: Authority to Collect

The Virginia Department of Social Services (VDSS), in compliance with 45 CFR §155.260, creates, collects, uses, maintains, and discloses ***Personally Identifiable Information (PII)*** based on the following federal authorizations:

- Sections 1137, 453, and 1106(b) of the Social Security Act (42 U.S.C. §§ 1320B-7, 653 and 1306(b)) (income and eligibility verification data);
- 26 U.S.C. § 6103(1)(7) and (8) (tax return data);
- Section 202(x)(3)(B)(iv) of the Act (42 U.S.C. § 402(x)(3)(B)(iv))(prisoner data);
- Section 1611(e)(1)(I)(iii) of the Act (42 U.S.C. § 1382(e)(1)(I)(iii)(Supplemental Security Income (SSI));
- Section 205(r) (3) of the Act (42 U.S.C. § 405(r) (3)) and the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, § 7213(a)(2)(death data);
- Sections 402, 412, 421, and 435 of Pub. L. 104-193 (8 U.S.C. §§ 1612, 1622, 1631, and 1645)(quarters of coverage data);
- Children's Health Insurance Program Reauthorization Act of 2009 (CHIPRA), Pub. L. 111-3 (citizenship data);
- Routine use exception to the Privacy Act, 5 U.S.C § 522a(b)(3) (data necessary to administer other programs compatible with SSA programs); and
- Patient Protection and Affordable Care Act of 2010 (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act (Public Law 111-152).

VDSS, in compliance 45 CFR §155.260, creates, collects, uses, maintains, and discloses ***PII*** based on the following state authorizations:

- *Code of Virginia* §63.2 State Welfare Programs (covers authority to collect and disclosure restrictions) for all programs managed by VDSS;
- *Code of Virginia* §63.2-104 Social Services Welfare data collection, disclosure; and
- *Code of Virginia* § 63.2-1246. Disposition of reports; disclosure of information as to identity of birth family.

AP-1: Purpose Specification

PII is needed to determine benefits eligibility for the programs listed in applicable state and federal data sharing agreements.

Data received from federal agencies is used to verify and validate information supplied by clients, household members, parents, non-custodial parents, and others in support of the administration and processing of applications and cases for benefits and services including Medical Assistance, Supplemental Nutrition Assistance Program (SNAP), Energy Assistance, Temporary Assistance for Needy Families (TANF), Child Support Enforcement, and other business critical systems.

AR: Governance and Privacy Program

Roles and Responsibilities

A. Commissioner

The Commissioner is responsible for ensuring the ***privacy*** of ***PII*** contained within VDSS information systems and data including case records and documents containing client or ***confidential*** information. The Commissioner, through the Information Security and Risk Management (ISRM) Office, is responsible for assuring that the VDSS Privacy Policy and Program Manual is developed and distributed to all VDSS divisions/directorates/offices/districts/regions and Local Departments of Social Services (LDSS) staff, contractors, vendors, and other persons and organizations that have a need to use VDSS-related information and information processing systems. The Commissioner is responsible for final interpretation of this VDSS Privacy Policy and Program Manual.

B. VDSS Privacy Officer

The Agency Chief Information Security Officer (CISO) of the Information Security and Risk Management Division (ISRM) has been designated as the VDSS Privacy Officer.

Barry Davis, CISSP
Agency Chief Information Security Officer
Agency Privacy Officer

Barry.Davis@dss.virginia.gov

801 E. Main Street, 7th Floor
Room 706
Richmond, Virginia 23219

Office: (804) 726-7153
Fax: (804) 726-7132

The VDSS Privacy Officer is accountable for developing, implementing, and maintaining the VDSS Privacy Policy and Program and governance to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of ***PII*** by programs and information systems.

The VDSS Privacy Officer monitors federal and state ***privacy*** laws for changes that affect the VDSS Privacy Policy and Program.

The VDSS Privacy Officer allocates appropriate budget and staffing resources to implement and operate the VDSS Privacy Policy and Program. The Information Technology (IT) Audit Manager has been designated as the VDSS Alternate Privacy Officer if the CISO is indisposed and a backup is needed. The ISRM Division staff is delegated responsibilities for the maintenance and implementation of the VDSS Privacy Policy and Program.

The VDSS Privacy Officer is responsible for developing a strategic organizational VDSS Privacy Policy and Program for implementing applicable ***privacy*** controls, policies, and procedures.

The VDSS Privacy Officer designates the IT Audit Manager the responsibility of evaluating compliance with identified ***privacy*** controls. The IT Audit Manager performs security reviews that assess ***privacy*** controls implemented over systems containing ***sensitive*** data.

The VDSS Privacy Officer is responsible for updating the VDSS Privacy Policy and Program when applicable ***privacy*** requirements change, at least biennially.

C. Information Security and Risk Management (ISRM) Office (Central Security Office)

The VDSS ISRM Office is responsible for providing technical information, security assistance, and fostering and overseeing the VDSS Privacy Policy and Program. Specific responsibilities are as follows:

a. Provide technical assistance to VDSS divisions/directorates/offices/districts/regions and LDSS in developing, implementing, and administering their Privacy Program and procedures;

b. Develop, maintain, and disseminate the VDSS Privacy Policy and Program and guidelines, ensuring their consistent interpretation and implementation throughout VDSS divisions/directorates/offices/districts/regions and LDSS;

c. Participate in VDSS system development activities to ensure an appropriate level of ***privacy***, ***integrity***, ***confidentiality,*** and ***availability*** is provided to VDSS systems;

d. Assist business areas to conduct Business Impact Analyses (BIAs) and Risk Assessments (RAs) for VDSS information systems;

e. Review VDSS Information Privacy Complaint Reports and coordinate Corrective Actions (CAs) to prevent similar occurrences;

f. Investigate alleged ***privacy*** breaches; and

g. Administer access privileges for *ALL* contract employees.

Note: The Commissioner and the VDSS Privacy Officer reserve the right and may assign other responsibilities as required to the ISRM Office.

D. State/Local Security Officers

State/Local Security Officers will be the default Local Privacy Officer unless the Director has appointed another person for this function. The Local Security/Privacy Officer is responsible to ensure that all users of VDSS information and information systems are made aware of the VDSS Privacy Policy and Program and receive continuing Information Security and Privacy Awareness Training.

See Section 2.5 State/Local Security Officers of the VDSS Information Security Policy and Program Guide.

E. Management

Managers at all levels are responsible for ensuring the ***privacy*** of ***PII*** contained within VDSS Information systems and data, including case records and documents containing client or ***confidential*** information under their jurisdiction. They shall take all reasonable actions to provide adequate security and to escalate problems, requirements, and matters related to ***privacy*** to the highest level necessary for resolution.

Division/directorate/office/district/regional management and LDSS directors are responsible to:

a. Appoint Primary and Backup State/Local Security Officers who will also be the default Local Privacy Officer. Directors cannot be State/Local Security Officers because of conflict with separation of duties. In order to maintain continuity of business operations, one Primary State/Local Security Officer and at least one Backup State/Local Security Officer should be trained and appointed for each State/Local office.

b. Implement and enforce procedures within their units which ensure compliance with VDSS information security policies and standards;

c. Ensure violations or suspected violations of the VDSS Privacy Program are reported to the VDSS CISO; and

d. Ensure that all users of VDSS information and information systems are made aware of the VDSS Privacy Policy and Program and receive continuing Information Security and Privacy Awareness Training.

F. System Owner (VDSS Division Directors)

The System Owner is the VDSS manager responsible for making system-related development and maintenance decisions and establishing priorities. With respect to ***privacy***, the System Owner's responsibilities include the following:

a. Require new employees complete Initial Information Technology Security Awareness Training in the Knowledge Center prior to, or as soon as practicable after, receiving access to the system, but within the first 30 days of employment;

b. Require that all information system users complete the required Annual Information Security and Privacy Awareness Training within the deadlines set by the ISRM Office;

c. Manage system risk and develop additional ***privacy*** policies, standards, and guidelines required to protect the system in a manner commensurate with risk;

d. Maintain compliance with the VDSS Privacy Program in all information system activities;

e. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system; and

f. Designate a System Administrator for the system if the system is not administered by the Information Technology Partnership - currently Virginia Information Technologies Agency/Northrop Grumman (VITA/NG).

*See AR-7: Accounting of Disclosures of **Sensitive** Information and DM-2: Data Retention and Disposal for additional responsibilities of System Owners.*

G. Data Owner

The Data Owner is the VDSS manager responsible for the policy and practice decisions regarding data, including case records and documents containing client or ***confidential*** information. The Data Owner is responsible for the following:

a. Evaluate and classify sensitivity of the data with the assistance of the VDSS CISO;

b. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs with the assistance of the VDSS CISO;

c. Communicate data protection requirements to the System Owner;

d. Define requirements for access to the data; and

e. Approve Firewall requests.

H. Local Social Service Directors

LDSS Directors that enter data supplied by clients or client representatives into local systems are responsible for the ***privacy*** of the ***PII*** of the local information systems and ***confidential*** information contained therein. LDSS Directors will ensure that ***PII*** or ***sensitive*** data from DSS systems stays inside those systems of record. The LDSS Director is responsible for assuring that the VDSS Privacy Policy and Program Manual is distributed to all LDSS staff, contractors, vendors, and other persons and organizations that use local systems that process or store VDSS-provided information. The LDSS Director is responsible for final interpretation of local ***privacy*** policies and procedures and will provide to the VDSS ISRM Office copies of all local information ***privacy*** policies and procedures.

The LDSS Director's data ownership responsibilities include:

a. Establish and maintain an Privacy Program for local systems that process or store client or VDSS-provided information (i.e., Harmony, EZ-filer) that includes:

    1. Privacy policies and standards distributed to all individuals who use local systems that process or store VDSS-provided information; and

    2. An Information Security and Privacy Awareness Training Program relevant to local systems.

b. Provide physical and logical separation of duties by ensuring no one person that has the ability to influence funds has sole control of ***sensitive*** processes.

I. All Personnel

All personnel, including VDSS employees, LDSS employees, contractors, volunteers, student interns, business partners, and any other users of VDSS information systems and resources are responsible for the following:

a. Read the VDSS Privacy Policy and Program Manual, the VDSS Information Security Policy and Program Guide, the VDSS Information Resource Acceptable Use Policy, and related information security policies, standards, and procedures;

b. Read and sign the VDSS Information Security – Policy Acknowledgement form;

c. Comply with the VDSS Privacy Policy and Program Manual, the VDSS Information Security Policy and Program Guide, the VDSS Information Resource Acceptable Use Policy, and related information security policies, standards, and procedures;

d. Do everything reasonably within their power to ensure that the VDSS Privacy Policy and Program Manual, the VDSS Information Security Policy and Program Guide, the VDSS Information Resource Acceptable Use Policy are implemented, maintained, and enforced;

e. Report breaches of ***privacy*** of ***PII***, actual or suspected, to the VDSS CISO and to appropriate management;

f. Take reasonable and prudent steps to protect the ***privacy*** of ***PII*** and ***confidential*** data to which they have access; and

g. Complete required Information Security and Privacy Awareness Training as required within specified deadlines.

    1. Initial Information Security Awareness Training must be completed within 30 days of employment. Employees in good standing who move from one LDSS office to another

LDSS office are not required to complete the Initial Information Security Awareness Training within 30 days of the transfer. A worker in "good standing" has no account suspensions or locks and has completed the most recent Annual Information Security and Privacy Awareness Training.

2. Annual Information Security and Privacy Awareness Training must be completed within the deadline as broadcast by the ISRM Office yearly.

3. Local Security Officer Training must be completed within 30 days of appointment and once every three years thereafter.

Related References:

VDSS Information Resource Acceptable Use Policy (.pdf)

VDSS Information Security - Policy Acknowledgement form (.pdf)

VDSS Information Security Policy and Program Guide (.pdf)

J. System Administrator

The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrators assist agency management in the day-to-day administration of VDSS information systems, and implement ***privacy*** controls and other requirements of the VDSS Privacy Program on information systems for which the System Administrator has been assigned responsibility.

The Division of Information Systems (DIS) and VITA are the System Administrators.

K. Data Custodian

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

a. Protect the data in their possession from unauthorized access, alteration, or destruction;

b. Establish, monitor, and operate information systems in a manner consistent with the VDSS Privacy and Policy Program, standards, and procedures; and

c. Provide Data Owners with reports, when necessary and applicable.

Note: NG is the Data Custodian for all VDSS data that resides on VITA/NG managed devices.

AR-1 Privacy Impact and Risk Assessment

The VDSS Privacy Officer or designee is responsible for documenting and implementing a Privacy Risk Management process. The Privacy Risk Assessment framework is included in the ISRM Risk Assessment process. An appendix relating to ***privacy*** controls is attached to a Risk Assessment framework if the system is classified as having ***sensitive***, ***privacy***-related, and ***PII*** data. The Risk Assessment Privacy control section assesses a sample of National Institute of Standards and Technology (NIST) ***privacy*** controls applicable to the system evaluation.

The VDSS Privacy Officer or designee conducts Privacy Impact Assessments (PIA) for information systems, programs, and other VDSS activities that pose a risk to the ***privacy*** of ***PII***. VDSS updates PIAs when there are significant changes to the VDSS Privacy Program or IT systems, when new ***PII*** data elements are added to the system, when existing ***PII*** data elements are to be removed from the system, or when there are changes to data-sharing policies or agreements that may change the VDSS Privacy Risk Profile.

The VDSS Privacy Officer or designee uses the approved VDSS Unified PIA Template to evaluate the information system's risk to the ***privacy*** of ***PII***. The VDSS Unified PIA Guide provides procedures on how to implement the PIA Template Evaluation.

AR-2 Privacy Requirements for Contractors

Contractors and providers include, but are not limited to, information providers, information processors, and other organizations that provide information system development, information technology services, consumer assistance, business functions, and other outsourced applications, roles, and functions.

Contractors will conform to the requirements of this VDSS Privacy Program based on the role and level at which they are performing or supporting: users, data custodian support, System Owner/developer, or System Administrator.

The VDSS Privacy Officer will ensure that agency proposals, contracts, and Memorandums of Agreement (MOAs) include ***privacy*** requirements in the agreements or acquisition related documents.

AR-3 Privacy Monitoring and Auditing

The VDSS Privacy Officer or designee monitors the internal VDSS Privacy Policy and Program annually with the Risk Assessment annual re-evaluation and treatment plan assessment. The VDSS Privacy Officer or designee audits the internal ***privacy*** control policy every three years in line with audit policy requirements to review a ***sensitive*** system or program once every three years.

Tri-annual internal Risk Assessments of internal ***privacy*** policy and controls can include self-assessments or third-party audits that result in reports of compliance gaps identified in programs, projects, and information systems.

VDSS has implemented ***privacy*** considerations into the life cycle of ***PII***, programs, information systems, mission/business processes, and technology. All project managers, developers, and contractors are required to take role-based ***privacy*** awareness training and role-base System Development Life Cycle (SDLC) training.

The VDSS Privacy Officer or designee annually monitors and documents ***privacy*** laws, regulations, and policies for changing requirements and considerations.

The VDSS Privacy Officer or designee tracks programs, information systems, and applications that collect and maintain ***PII*** through the Data Classification Program. ***Sensitive*** systems involving ***PII*** are tracked through the COV CETR and ARCHER systems. ARCHER acts as a tracking system or repository to associate data types with ***sensitive*** information systems.

The VDSS Privacy Officer ensures ***PII*** is limited to a "need-to-know" basis by training users in ***PII*** requirements through the Information Security and Privacy Awareness Training Program. VDSS implements information security requirements of least privilege and separation of duties to ensure security access is limited to those users with a business need to access ***PII*** for their job responsibilities.

The VDSS Privacy Officer ensures ***PII*** is maintained and used only for the legally authorized purposes by monitoring and implementing corrective action plans of internal Risk Assessments, third-party audits, and internal audits.

AR-4: Information Security and Privacy Awareness and Training

The VDSS Privacy Officer or designee promotes a culture of ***privacy*** compliance through the implementation of an Information Security and Privacy Awareness Training Program.

The VDSS Privacy Officer or designee develops, implements, dissisminates, and updates annually a comprehensive Information Security and Privacy Awareness Training Strategy aimed at ensuring applicable personal understand ***privacy*** responsibilities and procedures.

The VDSS Privacy Officer or designee requires annually that applicable personnel having responsibility for ***PII*** or for activities that involve ***PII*** partake in role-based, Information Security and Privacy Awareness Training modules. Privacy Awareness slides are included in the Annual Information Security and Privacy Awareness Training required for all users.

The VDSS Privacy Officer or designee implements the training modules electronically through the

Knowledge Center. The targeted training will include slides promoting the culture of Privacy Awareness and include assessment quizes to test users.

AR-5: Privacy Reporting

VDSS is not a federal agency, therefore does not develop, disseminate, and update reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies. This ***privacy*** control is meant for Department-level reporting to OMB and Congress about the VDSS Privacy Program.

The VDSS Privacy Officer or designee reports ***privacy*** compliance to CMS for MARS-E 2.0 compliance tri-annually (e.g., 2013 and 2016). Privacy compliance is reported using the SSP, PIA, and external assessments.

AR-6: Privacy-enhanced System Design and Development

VDSS project managers, developers, contractors, and users are required to design information systems that support ***privacy*** functions with automated ***privacy*** controls.

To the extent feasible, when designing organizational information systems, VDSS employs technologies and system capabilities that automate ***privacy*** controls on the collection, use, retention, and disclosure of ***PII***.

The VDSS Privacy Officer or designee requires ***sensitive*** information systems to be audited once every three years. ***Sensitive*** information systems that support ***privacy*** functions or include ***sensitive privacy***-related data will be included in the ~~3~~ three year VDSS Information Security Audit Plan to maintain compliance with the 45 CFR §155.260, the Privacy Act (if applicable) and the VDSS Privacy Policy.

AR-7: Accounting of Disclosures of *Sensitive* Information

System Owners or designees keep an accurate accounting of disclosures of information held in each system of record~~s~~, including:

- Date, nature, and purpose of each disclosure of a record; and
- Name and address of the person or agency to which the disclosure was made.

System Owners or designees, and ISRM retain the accounting of disclosures for the life of the record or five years after the disclosure is made, which is longer.

VDSS will provide the accounting of disclosures available to the person named in the record upon request.

DI: Data Quality and *Integrity*

VDSS takes reasonable steps to confirm the accuracy and relevance of ***PII***. Such steps may include editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the ***PII***, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of ***PII*** that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less ***sensitive PII***. Additional steps may be necessary to validate ***PII*** that is obtained from sources other than individuals or the authorized representatives of individuals. When ***PII*** is of a sufficiently ***sensitive*** nature (e.g., when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit), VDSS incorporates mechanisms into information systems and develops corresponding procedures for how frequently, and by what method, the information is to be updated.

DI-1: Data Quality

VDSS:

a. Incorporates detailed procedures for case and client workers, and uses automated verification techniques to confirm, to the greatest extent practicable upon collection or creation of ***PII***, the accuracy, relevance, timeliness, and completeness of that information;

b. Collects ***PII*** directly from the individual in–person, or through the online CommonHelp site where applicants enter the information themselves;

c. System and Data Owners check for, and correct as necessary, any inaccurate or outdated ***PII*** used by its programs or systems as directed by the Privacy Policy Program. The VDSS Data ***Integrity*** Board provides governance over data sharing and data management; and

d. Ensures and maximizes the quality, utility, objectivity, and ***integrity*** of disseminated information through information security and ***privacy*** policies, process manuals, and guidelines.

DI-2: Data Validation

VDSS:

a. Requests the user to validate ***PII*** during the collection process in web-based systems; and

b. Requests revalidation for accuracy when data is being updated either by the client, authorized representative, or caseworker.

DI-3: Data *Integrity* and Data *Integrity* Board

VDSS:

a. Ensures the ***integrity*** of ***PII*** through the use of access controls and user roles, the use of online verification and validation of data, and encryption techniques in the storage, transmission, and presentation of ***PII***.

b. Uses a Data ***Integrity*** Board that reviews Interface Agreements, Contracts, and Memorandums of Understandings (MOUs) that involve the exchange of ***PII***. The VDSS Data ***Integrity*** Board meets as needed and performs its functions either virtually through online or telephonic meetings, or in person. The VDSS Data ***Integrity*** Board consists of:

i. General Services Representative;

ii. CISO or designated representative;

iii. Chief Information Officer (CIO) or designated representative;

iv. Data Owner; and

v. System Owner.

DM: Data Minimization and Retention

VDSS ensures the collection of ***PII*** is consistent with a purpose authorized by law or regulation. The minimum set of ***PII*** elements required to support a specific organization business process may be a subset of the ***PII*** the organization is authorized to collect. Program officials consult with the VDSS Privacy Officer and legal counsel to identify the minimum ***PII*** elements required by the information system or activity to accomplish the legally authorized purpose.

DM-1: Minimization of *Personally Identifiable Information* (*PII*)

VDSS:

a. Identifies the minimum ***PII*** elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

b. Uses the VaCMS to limit the collection and retention of ***PII*** for agency programs to the minimum elements identified, for the purposes described in the notice, and for which the individual has provided consent;

c. Conducts an initial evaluation of ***PII*** holdings, and periodically reviews the holdings, within every 365 days, to ensure that only ***PII*** identified in the notice is collected and retained, and that the ***PII*** continues to be necessary to accomplish the legally authorized purpose, as part of a Data Classification Review; and

d. Uses tools like Oracle Audit Vault to redact, de-identify, or mask specified ***PII*** to reduce risk resulting from disclosure (DM-2).

DM-2: Data Retention and Disposal

The VDSS Privacy Officer or designee requires that System Owners locate and remove/redact specified ***PII*** and/or use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

System Owners consult with the VDSS Privacy Officer and legal counsel to identify the minimum ***PII*** elements required by the information system or activity to accomplish the legally authorized purpose.

System Owners, in collaboration with the VDSS Privacy Officer, conduct an initial evaluation of ***PII*** holdings, and periodically review the holdings, within every 365 days, to ensure that only ***PII*** identified in the notice is collected and retained, and that the ***PII*** continues to be necessary to accomplish the legally authorized purpose.

The VDSS Information Security Policy and Program Guide states:

a. Federal data and CMS related case data, reports, and logs should be retained for ten years;

b. FTI should be destroyed after use or according to the VDSS record retention schedule; and

c. All other ***sensitive*** information, including internal inspection records, must be retained for three years or until audited or until no longer administratively useful.

Centers for Medicare and Medicaid Services (CMS) further requires the following ***privacy*** constraints:

a. Retain each collection of ***PII*** for the minimum allowable time period necessary to fulfill the purpose(s) identified in the notice or as required by law;

b. Dispose of, destroy, erase, and/or anonymize the ***PII***, regardless of the method of storage, in accordance with a National Archives and Records Administration (NARA) - approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

c. Use legally compliant techniques or methods to ensure secure deletion or destruction of ***PII*** (including originals, copies, and archived records).

VDSS is required to:

- Configure information systems to record the date ***PII*** is collected, created, or updated and when ***PII*** is to be deleted or archived under a record retention schedule; and

- Where feasible, use~~s~~ techniques to minimize the risk to ***privacy*** of using ***PII*** for research, testing, or training.

VDSS:

a. Retains each collection of ***PII*** to fulfill the purpose(s) identified in the notice or as required by law;

b. Disposes of, destroys, erases, and/or anonymizes the ***PII***, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

c. Uses legally compliant techniques or methods to ensure secure deletion or destruction of ***PII*** (including originals, copies, and archived records).

*NOTE: VDSS uses the EAL to record when **PII** is added, updated, and viewed.*

DM-3: Minimization of *PII* used in Testing, Training, and Research

VDSS:

a. Through this policy, prohibits the use of ***PII*** for system testing, training, and research;

b. Implements controls to protect ***PII*** used for testing, training, and research;

c. Uses known data sources only (i.e., client-provided, federal/state agency sourced, third party provided - CheckPoint or LexisNexis, etc.);

d. Distributes non-***sensitive*** data with little or no restriction;

e. Allows ***PII*** distribution with client consent in certain cases; and

f. Ensures research beneficiaries and research data recipients protect ***PII*** data to federal and state standards.

IP: Individual Participation and Redress

VDSS may obtain consent through three methods: opt-in consent, opt-out consent, or implied consent.

Opt-in consent is the preferred method, but it is not always feasible. Opt-in consent requires individuals take affirmative action to allow organizations to collect or use ***PII***. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent.

In contrast, opt-out consent requires individuals to take action to prevent the new or continued collection or use of such ***PII***.

Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of ***PII*** (i.e., posted signs/notices). Examples of implied consent are:

- VDSS' application process utilizes click-to-consent.
- Electronic signature through the application process or CommonHelp website.
- Wet signature or hand-written signature on a paper application.
- Call Center uses telephonic signature through verbal consent.
- Authorized representative consent can happen through any of the above methods as a proxy.

IP-1: Consent

VDSS:

a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of ***PII*** before its collection;

b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, or retention of ***PII***;

c. Obtains consent, where feasible and appropriate, from individuals before any new uses or disclosures of previously collected ***PII***;

d. Ensures individuals are aware of and, where feasible, consent to all uses of ***PII*** not initially described in the public notice that was in effect at the time the organization collected the ***PII***; and

e. The organization implements mechanisms to support itemized or tiered consent for specific uses of data.

IP-2: Individual Access

VDSS:

a. Provides individuals the ability to have access to their ***PII*** maintained in its system(s) of record~~s~~;

b. Publishes access procedures; and

c. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

IP-3: Redress

VDSS:

a. Provides information to individuals concerning how to contact the relevant organization to have inaccurate ***PII*** maintained by that organization corrected or amended, as appropriate; and

b. Establishes a process for disseminating corrections or amendments of the ***PII***, if the inaccurate ***PII*** was maintained solely by the organization, to other authorized users of the ***PII***, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

IP-4: Complaint Management

VDSS is required to implement a process for receiving and responding to complaints, concerns, or questions from individuals about VDSS ***privacy*** practices.

Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and ***privacy*** and security safeguards.

VDSS must provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints, and are easy to use. VDSS is required to respond to complaints, concerns, and questions from individuals within a reasonable time period.

VDSS implements multiple avenues to voice client and customer complaints. Clients can utilize the Department of Medical Assistance Services (DMAS) appeal process if they are dissatisfied with VDSS dispositions.

Clients can contact VDSS home office, their locality, or the DMAS call center to make changes to their ***PII***.

Once the changes are made to ***PII***, VDSS will notify the client of a change with a notice. If there is a case review in question, a corrective action plan can be implemented.

VDSS Information Privacy Complaint Process

Anyone can file a VDSS Information Privacy Complaint. Privacy complaints will be processed in accordance with VDSS Public Affairs, Citizen Service's timeline of 5 business days. The VDSS Information Privacy Complaint Form must be completed and:

- Be filed in writing by mail, fax, or email.
- Name the covered entity or client involved, and describe the acts or omissions, believed to have violated the VDSS Privacy Program or the VDSS Information Security Program.
- Be filed within 180 days of the date that knowledge of the act or omission occurred. VDSS may extend the 180-day period for "good cause."

Related Reference:

VDSS Information Privacy Complaint Form (.pdf)

SE: Security

The VDSS uses the Data Classification process to maintain and update the inventory of programs, systems, and devices used for collecting, creating, using, disclosing, maintaining, or sharing ***PII***.

VDSS:

a. Establishes, maintains, and updates within every 365 days, an inventory of all programs and systems used for collecting, creating, using, disclosing, maintaining, or sharing ***PII***; and

b. Provides each update of the ***PII*** inventory to the organization's designated ***privacy*** official or information security official to support the establishment of information security requirements for all new or modified information systems containing ***PII***.

c. The VDSS Privacy Incident Response is integrated into the VDSS Information Security Incident Response Plan (SE-2).

TR: Transparency and Notifications

Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how VDSS uses ***PII*** generally and, where appropriate, to make an informed decision prior to providing ***PII*** to VDSS.

Effective notice also demonstrates the ***privacy*** considerations VDSS has addressed in implementing its information practices.

General public notice and direct notice to individuals may be provided through a variety of means including System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website ***privacy*** policy, as required by applicable law and policy.

The VDSS Privacy Officer or designee is responsible for the content of the VDSS public notices, in consultation with legal counsel and relevant program managers.

TR-1: VDSS Privacy Notice

VDSS only collects personal information to the extent necessary to provide services or benefits. VDSS does not sell or rent user information to any outside company or organization. VDSS does not reveal

specific information about users to third parties for their independent use, except if required to do so by the Virginia Freedom of Information Act (FOIA).

VDSS:

a. Provides effective notice to the public and to individuals regarding:

   1. Activities that impact ***privacy***, including its collection, use, sharing, safeguarding, maintenance, and disposal of ***PII***;

   2. Authority for collecting ***PII***;

   3. The choices, if any, individuals may have regarding how the organization uses ***PII*** and the consequences of exercising or not exercising those choices; and

   4. The ability to access and have ***PII*** amended or corrected if necessary.

b. Describes:

   1. The ***PII*** the organization collects and the purpose(s) for which it collects that information;

   2. How the organization uses ***PII*** internally;

   3. Whether the organization shares ***PII*** with external entities, the categories of those entities, and the purposes for such sharing;

   4. Whether individuals have the ability to consent to specific uses or sharing of ***PII*** and how to exercise any such consent;

   5. How individuals may obtain access to ***PII***; and

   6. How the ***PII*** will be protected.

c. Revises its public notices to reflect changes in practice or policy that affect ***PII*** or changes in its activities that impact ***privacy***, before, or as soon as practicable after the change.

d. Provides real-time notice using CommonHelp.

e. Ensures public access to information about its ***privacy*** activities and is able to communicates with its designated ***privacy*** official by publishing this information on the VDSS public site, SPARK, etc.

UL: Use Limitation

VDSS uses ***PII*** only for the purposes identified in the Privacy Act or in public notices.

UL-1: VDSS Internal Use Policy Statement

VDSS will only use ***PII*** internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

VDSS is required to take steps to ensure proper ***PII*** use.

These steps include monitoring and auditing organizational use of ***PII*** and training organizational personnel on the authorized uses of ***PII***.

UL-2: Information Sharing with Third Parties

VDSS:

a. Shares ***PII*** externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;

b. Where appropriate, enters into MOUs, MOAs, Letters of Intent, Computer Matching Agreements (CMAs), or similar agreements, with third parties that specifically describe the ***PII*** covered and specifically enumerate the purposes for which the ***PII*** may be used;

c. Monitors, audits, and trains its staff on the authorized sharing of ***PII*** with third parties and on the consequences of unauthorized use or sharing of ***PII***; and

d. Evaluates any proposed new instances of sharing ***PII*** with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.